ORIGINAL

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

'08 MJ 1330

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>SERGEY ALEXANDROVICH PAVLOVICH (1),<br>aka Panther,<br>aka Diplomaticos,<br>aka PoL1Ce Dog,<br>aka Fallen Angel,<br>aka Panther757,<br>DZMITRY VALERYEVICH BURAK (2),<br>aka Leon,<br>aka Graph,<br>aka Wolf,<br>SERGEY VALERYEVICH STORCHAK (3)<br>aka Fidel,<br><br>Defendants. | Criminal Case No. _____<br><br>C O M P L A I N T<br><br>Title 18, U.S.C., Secs. 1029(b)(2) - Conspiracy to Traffic Unauthorized Access Devices. |

The undersigned complaint, based upon the attached affidavit, and being duly sworn:

**Count 1**

**Conspiracy to Traffic in Unauthorized Access Devices**

Beginning on a date unknown and continuing up to and including April 28, 2008, within the Southern District of California, and elsewhere, defendant SERGEY ALEXANDROVICH PAVLOVICH, aka Panther, aka Diplomaticos, aka PoL1Ce Dog, aka Fallen Angel, aka Panther757,

DZMITRY VALERYEVICH BURAK, aka Leon, aka Graph, aka Wolf, SERGEY VALERYEVICH STORCHAK aka Fidel, with the intent to defraud, did knowingly and intentionally conspire together with each other and with other persons known and unknown, to:

a. knowingly and with intent to defraud, traffic in one or more unauthorized access devices, that had been stolen or obtained with the intent to defraud, and by such conduct affect interstate commerce and obtain anything of value aggregating $1,000.00 or more during that period; in violation of Title 18, United States Code, Sections 1029(a)(2) and (c)(1)(A)(i).

**OVERT ACTS**

In furtherance of the conspiracy, and to effect the objects thereof, the following overt acts, among others, were committed within the Southern District of California, and elsewhere:

a. On or about May 11, 2007, SERGEY ALEXANDROVICH PAVLOVICH, aka Panther, aka Diplomaticos, aka PoL1Ce Dog, aka Fallen Angel, aka Panther757, negotiated the sale of 90 stolen credit card account numbers with a purchaser located in the Southern District of California.

b. On or about September 11, 2006, DZMITRY VALERYEVICH BURAK, aka Leon, aka Graph, aka Wolf, negotiated the sale of 30 stolen credit card account numbers with a purchaser located in the Southern District of California.

c. On or about October 10, 2007, SERGEY VALERYEVICH STORCHAK, aka Fidel, agreed to sell 64 stolen credit

card account numbers to a purchaser located in the Southern District fo California.

All in violation of Title 18, United States Code, Section 1029(b)(2).

Ryan Knisely
Special Agent
Unites States Secret Service

Sworn before me and subscribed in my presence, April 28, 2008

HON. NITA L. STORMES
U.S. Magistrate Judge

## AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Ryan Knisley, being duly sworn, hereby declare and state as follows:

1. Your affiant is a Special Agent with the United States Secret Service ("USSS") and has been so employed in this capacity since August 7, 2006. During that time, I have received formal training in investigating counterfeit access device fraud and other financial crimes. I have received this training at the United States Secret Service Special Agent Training Course in Beltsville, Maryland and the Federal Law Enforcement Training Center in Glynco, Georgia. I am currently assigned to the San Diego Field Office and my primary assignment is the investigation of financial crimes. As a Special Agent with the USSS I am responsible for investigating violations of Title 18, United States Code, Sections 1028, 1029, 1342, 1343 and 1344.

2 I make this affidavit in support of a criminal complaint and arrest warrant against:

a. Sergey Alexandrovich Pavlovich ("**Pavlovich**"), aka *Panther*, aka *Diplomaticos*, aka *PoL1Ce Dog*, aka *Fallen Angel*, aka *Panther757*, a citizen of Belarus, for Conspiracy to Traffic in Unauthorized Access Devices in violation of Title18, United States Code, Section 1029(b)(2);

b. Dzmitry Valeryevich Burak ("**Burak**"), aka *Leon*, aka *Graph*, aka *Wolf*, a citizen of the Ukraine, for Conspiracy to Traffic in Unauthorized Access Devices in violation of Title18, United States Code, Section 1029(b)(2);

c. Sergey Valeryevich Storchak **("Storchak")**, aka Fidel, a citizen of the Ukraine, for Conspiracy to Traffic in Unauthorized Access Devices in violation of Title18, United States Code, Section 1029(b)(2).

3. The information set forth below is based upon my personal knowledge and/or information communicated to me from other law enforcement officers involved in the investigation of the aforementioned individual.

4. In May 2005, the USSS served a search warrant upon Yahoo! Inc. for an e-mail address used by **Burak**. As a result of this search warrant, the USSS discovered *inter alia* 82 saved e-mail messages between **Burak** and **Storchak.** These particular saved e-mail messages contained Bank Identification Number ("BIN") lists, stolen credit card account numbers and records of proceeds derived from the distribution of stolen credit card account numbers. Based upon my training and experience I know that BIN lists are essentially available inventory catalogues listing the type and quantity of credit card account numbers available for purchase. For example, a BIN list will generally contain the issuing bank's name and, often, the class of credit account represented (e.g., classic, gold, platinum, etc.) followed by the quantity of account numbers available within each category.

5. Additional search warrants served upon **Storchak's** Yahoo! Inc. e-mail account during July 2005 revealed additional saved e-mail messages between **Storchak** and **Burak**. These particular

saved e-mail messages revealed additional stolen credit card account numbers that were transferred between **Burak** and **Storchak**. Investigating agents also found several saved e-mail messages documenting the fact that **Storchak** was using the internet to distribute stolen credit card account numbers to end-users/purchasers located throughout the world. A preliminary financial analysis of the aforementioned e-mail messages from **Storchak**'s and **Burak**'s Yahoo e-mail accounts indicate that the credit card account numbers transferred between **Burak** and **Storchak** resulted in approximately US$7,000,000.00 in actual loss.

6. During April 16, 2008, pursuant to a Mutual Legal Assistance Treaty request to the State of Israel, the USSS received digital evidence from an Israeli based e-mail service provider called SAFe-mail. SAFe-mail provided saved e-mail messages belonging to e-mail accounts used by **Pavlovich** and **Burak**. These saved e-mail messages were, in turn, provided to the USSS.

7. The saved SAFe-mail e-mail messages provided to the USSS reveal that **Burak** regularly communicated with **Storchak** and several other individuals who were known to traffic in stolen credit card account information. Specifically, e-mail header information from each of these e-mail messages indicate that **Pavlovich** and **Burak** regularly sent and received e-mail messages with attachments to a variety of individuals who also traffic in stolen credit card account information. Moreover, **Pavlovich**'s SAFe-mail account contained numerous saved e-mail messages from **Burak**. These particular saved e-mail messages specifically reveal that **Pavlovich** and **Burak** transferred at least one BIN list and over six hundred stolen credit card account numbers to each other. Contained within one particular e-mail message, **Pavlovich** stated to **Burak** that a group of particular stolen credit card account numbers were particularly "reliable."

8. On September 9, 2004, Belarus law enforcement authorities seized a computer hard drive which belonged to **Pavlovich**. This hard drive was provided to the USSS and contained saved web-page files, saved e-mail messages pay-and-owe sheets and a variety of "registration type" files which allowed agents to learn that **Pavlovich** owned and administered the internet web-site, *www.DumpsMarket.net ("DumpsMarket")*. Evidence from **Pavlovich**'s hard drive revealed that *DumpsMarket* hosted a members-only forum where carders could openly interact and conduct carder-related business with one another. Additional saved-e-mail messages revealed that **Pavlovich** would also use *DumpsMarket* to facilitate his own personal sales of stolen credit card account numbers.

9. The *DumpsMarket* web-site itself identified **Pavlovich** as the proprietor and listed **Burak** as an administrator. Additional evidence from **Pavlovich**'s hard drive revealed that in addition to web-site administrators, *DumpsMarket* utilized the services of Tested Vendors. Tested Vendors were individuals who had proven their status as accomplished and reliable carders and who were allowed to sell stolen credit card account numbers on *DumpsMarket*. Based on saved e-mail massages and logged chat sessions, Tested Vendors worked directly for **Pavlovich** who provided them with stolen credit card account numbers and were tasked to sell these account numbers to *DumpsMarket* members/end users. **Storchak** was listed on the *DumpsMarket* web-site as a Tested Vendor. The pay-and-owe sheets recovered from the drive indicate that **Pavlovich** would thereafter receive a majority cut from the sale of each stolen credit card account number.

10. Based upon a forensic examination of **Pavlovich**'s hard drive and my training and experience in the investigation of individuals who traffic in stolen credit card account information, I learned that *DumpsMarket* members/end users communicated with the Tested Vendors primarily *via* ICQ chat and e-mail messages. Generally, sales and purchases were solicited and initiated on *DumpsMarket's* forums. Transaction details were subsequently negotiated and agreed upon *via* ICQ chat sessions. Stolen credit card account numbers were then generally sent to the purchaser *via* ICQ message or an e-mail message attachment.

11. **Pavlovich**'s hard drive also contained approximately 10,000 stolen credit card account numbers. Moreover, the same hard drive contained numerous photographs of **Pavlovich**, **Burak** and **Storchak** spending time with one another in various social settings.

12. Saved e-mail messages and logged instant-chat sessions indicate that **Pavlovich**, **Burak** and **Storchak** each negotiated the sale and actually sold stolen credit card account numbers to a purchaser located within the Southern District of California. Specifically, on or about May 11, 2007 **Pavlovich** sold 90 stolen credit card account numbers to an individual in the Southern District of California. Similarly, on September 11, 2006, **Burak** sold approximately 30 stolen credit card account numbers to a purchaser in the Southern District of California. Finally, on October 10, 2007 **Storchak** sold 64 stolen credit card account numbers to a purchaser located in the Southern District of California. Each of the aforementioned sales resulted in a transfer of stolen credit card account numbers to the Southern District of California where the aforementioned purchaser was located.

13. Based upon the saved e-mail messages taken from 1) **Burak**'s Yahoo! e-mail account, 2) **Storchak**'s Yahoo! e-mail account, 3) and **Pavlovich**'s hard drive, I believe that **Pavlovich**, **Burak** and **Storchak** conspired with each other and others known and unknown to distribute stolen credit card account information in the Southern District fo California. Moreover, given the evidence discovered on **Burak**'s and **Pavlovich**'s SAFe-mail accounts and the sales to a purchaser in the Southern District of California, I believe that **Pavlovich**, **Burak** and **Storchak** are currently still conspiring to distribute stolen credit card account information.

14. Based on the above facts, I believe there is probable cause that **Pavlovich**, **Burak**, and **Storchak** violated Title 18, United States Code, Section 1029(b)(2), Conspiracy to Traffic in Unauthorized Access Devices

15. Because this Affidavit is being submitted for the limited purpose of establishing probable cause sufficient to support a criminal complaint, I have not set forth each and every fact learned during the course of this ongoing investigation. Rather, I have set forth only those facts that I believe are necessary to establish the foundation for a criminal complaint.

RYAN KNISLEY
SPECIAL AGENT, UNITED STATES SECRET SERVICE